

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA)	
)	
v.)	Crim. No. 01-455-A
)	
ZACARIAS MOUSSAOUI)	

DECLARATION OF DONALD EUGENE ALLISON

1. My name is Donald Eugene Allison. I am a computer forensics practitioner in private practice in Richmond, VA. I have worked in computer forensics for approximately three years, and in information technology for over seventeen years. I am a member of the High Technology Crime Investigation Association ("HTCIA"), Mid-Atlantic Chapter. I am currently on the faculty of the Virginia Institute for Forensic Science and Medicine, as a computer forensics lecturer. I also work as a contractor to the United States Missile Defense Agency, Systems Engineering Verification division. In addition, I have received training in computer forensics investigations of networked and standalone systems, Microsoft Windows, Apple Macintosh, Unix, and Linux operating systems, as well as portable digital assistants. This training has been through private companies as well as through the law enforcement, government, and military members of the HTCIA.

2. Before my current work in forensics, I was contracted to support the Missile Defense Agency, Test and Evaluation Division in developing Information Assurance policy. For two years prior to that time, I worked with the Office of the Secretary of Defense, Joint Test and Evaluation, Joint Warfighters group as the computer simulations expert. Five years prior to that time I worked as a contractor to

the U.S. Joint Forces Command and the Joint Warfighters Center as the Navy Joint Simulation controller. Also, I spent five years at Johns Hopkins University, Applied Physics Laboratory, as a researcher. Prior to Hopkins, I worked as a contractor to NASA's Goddard Space Flight Center, and as an analyst at the Skidaway Institute of Oceanography, Savannah, GA.

3. I have extensive experience in data analysis, computer programming, systems administration, network design, system security, incident response, and international operations. My educational background is in meteorology with a Masters Degree from the Florida State University, and a Bachelors Degree from Pennsylvania State University.

4. I have been retained by the Federal Public Defender, Eastern District of Virginia, for case Cr. No. 01-455-A, *United States v. Zacarias Moussaoui*. I have or am in the process of performing forensic evaluations of hard drives delivered in discovery, including those for Mr. Moussaoui's laptop, the University of Oklahoma ("UO") system, and Mr. Mukkarum Ali's laptop.

5. On September 5, 2002, I was asked to review the affidavit supplied by FBI Special Agent Bridget A. Lawler dated September 4, 2002 (the "Lawler Affidavit"), regarding the investigation procedures for Hotmail accounts allegedly used by Mr. Moussaoui. Below is a review of my findings.

General Observations

6. There is a general concern with this case regarding the authenticity of the hard drives given to the defense as part of discovery. To the best of my knowledge, and with the one exception noted below, the government has yet to provide the

authentication information regarding the copies made of the original hard drives, including those for Mr. Moussaoui's laptop, the Oklahoma University system, and Mr. Mukkarum Ali's laptop. This authentication information (such as the MD5 message digest and other accepted computer forensic methods) is critical as without it, it is impossible to verify that the duplicate hard drives are an exact copy of those that exist on the original systems. Likewise, without such information it is impossible to determine if the material retrieved from the hard drives is accurate.

7. In this regard, I have reviewed two documents, a copy of which is attached, each dated August 6, 2002, referenced by Bates nos. M-LBR-70002263 through 2265. According to a September 9, 2002 letter to the defense from the government, copy also attached, the above documents constitute the authentication information for Mr. Moussaoui's laptop. With all respect to the government, the referenced documents do not constitute sufficient authentication for the laptop. Such information should include documentation that shows that the hard drive in the laptop is an exact duplicate of the original drive seized by the government. Many methods are available to create an exact duplicate; however, only one method - the GNU/Linux routine dd - has been approved by the National Institute of Standards and Technologies. Further, once the duplicate has been created, a product such as the Message Digest version 5 (MD5) or the Secure Hash Algorithm version 1 (SHA-1) should be used to confirm that the duplication process has been done properly. The referenced documents do not contain any of the above documentation/information.

8. The complete authentication information for Mr. Moussaoui's laptop is even more critical given the indication in the above documents, particularly Bates no.

M-LBR-0002265, that the laptop had lost all power by the time of the government's CART examination on August 6, 2002.¹ The loss of all power means that the original date and time settings cannot be retrieved, and that other settings, such as how the computer performed its boot sequence, the types of ports and peripherals enabled, and the settings regarding the hard disk and the controller, are all lost as well. All of this is essential information on how the laptop was set up.

9. The authentication information also could clear up a concern I have regarding the copy provided to the defense of the University of Oklahoma hard drive. The hard drive delivered in discovery contains 80 gigabytes of storage area. However, the data from the UO system only comprises approximately 10 GB of storage area.² That leaves approximately 70 GB of storage area that should be empty. However, my review of that 70 GB area revealed that it was not empty, but rather, contained material that should not be there. This leads me to question whether the UO hard drive may be contaminated.³

10. Regarding Special Agent Lawler's affidavit, my specific concerns are as follows:

¹ If the August 6, 2002 reports (Bates nos. M-LBR-70002263 through 2265) constitute the only authentication information of the laptop, it defies reason why the government waited until then to gather such information on a laptop that has been available for analysis since September 11, 2001.

² My examination revealed that the hard drive contained a 10 GB partition that was useable to users and a 70 GB area that was flagged as unuseable.

³ It also forced me to examine 70 GB of unused storage space in addition to the 10 GB of relevant data. Had the information been provided to me on a 15 GB hard drive, my examination of the hard drive would have taken much less time.

Ref. xdesertman@hotmail.com Account and Other Email Accounts

A. Paragraph 10 (page 3-4): Special Agent Lawler states that a user must proactively download information from a Hotmail account in order for a message to be retained on the user's system. This is definitely not the case for the computers in question. A computer uses a program called a browser which allows the user to be able to access the internet in the point and click environment. As part of the design of the browser software, temporary files are created by the software in order to operate properly. Those temporary files include the "cache files" mentioned in Paragraph 11 of the Lawler Affidavit. These temporary files are created without the user proactively downloading any specific message information, and are available on the system until they are overwritten. Thus, contrary to what the Lawler Affidavit implies, useful information can be obtained from a computer even though the computer user has not proactively downloaded information from a Hotmail account.

B. Paragraphs 14 and 33 (pages 5 and 13-14): Special Agent Lawler describes the "relatively small chance that a random remnant of memory still extant in a computer's hard drive or temporary file will include the Hotmail account name. In my experience, and based on discussions with other FBI computer experts, such a find is very, very rare." See Lawler Affidavit at ¶ 14. I disagree with this conclusion. As noted previously (see ¶ 10.A above), temporary files are created on a hard drive even though the user has not proactively downloaded information from a Hotmail account. Information can be extracted from these temporary files. For example, on the laptop allegedly owned by Mr. Ali, I found material from three different Hotmail accounts that included information about mailbox contents as well as email messages themselves.

All of this material came from temporary files. (The search for this material took a relatively short period of time, and is just an example of the information available to an investigator who takes the time to mine the temporary files.) In addition, I identified nine distinct web-based email accounts on this laptop, most of which came from those “very, very rare” random remnants. (I did not, however, find any reference to xdesertman, but partial emails from that account may still reside on the laptop.) Thus, it is not rare, but very likely that information would be found in temporary files referring to email accounts. This includes not just information related to xdesertman, but also to all of the email names listed in paragraph 33 of the Lawler Affidavit.

There also is no indication in the Lawler Affidavit that the government’s search extended beyond Hotmail to organizations with which it shares account information. For example, Hotmail, which is a subsidiary of Microsoft, has relationships with other Microsoft divisions as well as with companies such as Infospace, which publishes a white pages style email phonebook for the internet. Pursuant to those relationships, when a Hotmail email account is opened, information about that account is sent to other Microsoft divisions and Infospace automatically unless the account holder affirmatively indicates that he/she does not want such information to be shared. Such information could include not only the account name, but also the holder’s place of residence, address, and other personal information. A truly thorough search for account information for xdesertman and the other accounts referenced in paragraph 33 of the Lawler Affidavit should include a search of the other Microsoft divisions as well as third-party companies.

Ref. Pilotz123@hotmail.com and the University of Oklahoma Computer

C. Paragraph 20, Item 4 (page 8) and paragraph 27 (page 12): The Lawler Affidavit states that “[f]rom a review of the Hotmail internet protocol address connection log for the pilotz123@hotmail.com account, agents were able to determine that Moussaoui connected to the internet to check his email from the following five separate computers/locations.” The Affidavit then goes on to list “PC 11” at UO as one of those computers. The Affidavit lists the Internet Protocol (IP) address for that computer as 129.15.157.31. (This address is the primary identification address for that computer on the internet.) However, when discussing this same computer in Paragraph 27 (page 12), the Affidavit identifies PC 11 not with the above IP address, but with a different one: 129.15.110.31. Given this discrepancy, I cannot determine whether, based on the Lawler Affidavit, the government has examined the correct computer from which Mr. Moussaoui allegedly connected to the internet to check his email. In this regard, the 80 GB hard drive produced in discovery referenced in paragraph 9 above, has an IP address of 129.15.110.31. Accordingly, it appears that the government obtained a hard drive other than the one used by Mr. Moussaoui at UO.⁴

⁴ Both IP 129.15.157.31 and 129.15.110.31 are valid IP addresses belonging to the University. The differing numbers (157 and 110) refer to subnets set up inside of the University network. The 157 subnet is assigned to the apartment complex where Mukkarum Ali’s computer was plugged in. The 110 subnet is assigned to the lab complex in the University’s student union. It is feasible that a computer could be called “PC11” and be located at either of these subnets. The hard drive that I examined from UO had the name LN-OMU-PC11, indicating that it came from the lab complex in the student union. The UO hard drive referenced in the Lawler Affidavit, however, is merely identified by “PC 11” making it difficult to determine if the correct hard drive was seized. Moreover, the hard drive referenced in paragraph 20(4) of the Lawler Affidavit has a subnet address of 157, which, as indicated, is inconsistent with

Ref. Kinko's, Eagan, Minnesota

D. Paragraphs 22-23 (pages 9-10): Special Agent Lawler states that the system from Kinko's in Eagan, Minnesota was not seized due to the data being erased every twenty-four hours. In order to better understand what this means, more information regarding the procedures used by Kinko's and the steps the Kinko's staff took to clean its system is needed. For example, if the process results in only selected portions of the hard drive being cleaned, which is often the case, then information related to user activities may still exist on the non-cleaned portions of the drive. Thus, unless the *entire* disk is routinely cleaned during the cleaning process, there is an excellent chance that temporary files are still resident on the system that may provide valuable information.

Ref. Mukkarum Ali's Computer

E. Paragraph 26 (page 11): Special Agent Lawler states that "[a]s a part of the review . . . agents looked for all files created, modified, or deleted on the dates we suspected that Moussaoui used Ali's computer." Searching by those dates is certainly one way to search for relevant data. However, relevant data can also reside in "file slack" portions of Mr. Ali's computer. These are files that have been partially overwritten by other information, and do not necessarily have dates associated with them.⁵ Thus, searching only by a date would not necessarily pull up helpful data extant

that paragraph's assertion that PC11 was located in "a University computer lab."

⁵ Files created on a hard disk are stored in fixed length records on the disk by the operating system. Rarely do file sizes exactly match the size of the fixed record lengths used by the operating system. The data storage space that exists from the end of the actual information in that file to the last boundary of the record length assigned to


on a file slack portion of Mr. Ali's computer.

Ref. the University of Oklahoma Computer

F. Paragraph 28 (page 12): Special Agent Lawler claims that the likely loss of information regarding Mr. Moussaoui was due to the "ghosting" performed by UO personnel. Assuming that the government is examining the correct hard drive (given the different IP addresses listed in the Lawler Affidavit, see ¶ 10.C above), it is critical to know the procedures employed by those personnel before the conclusion can be drawn that "any forensic evidence showing use of that computer by Moussaoui . . . was likely lost during [the] ghosting process." Lawler Affidavit at ¶ 28. For example, it is important to know what the settings were and the procedures used during the ghosting process. The use of Symantec's Norton Ghost software, for instance, does not automatically use wiping as part of its process. This must be done by utilizing the GDISK utility that is included with the Norton Ghost software but is separately activated. (Alternatively, one could use another product that specifically is used to wipe the disk entirely clean.) My own review of the UO hard drive (129.15.110.31) found temporary files dated from July 2001 thru August 2001. These files should not be there if the hard drive had been *entirely* wiped clean on August 30, 2001 by the ghosting process. Thus, it may be that forensic evidence of Mr. Moussaoui's use of the UO computer may still be retrievable from the UO hard drive despite the Lawler Affidavit's statement that such evidence was "likely lost" during the ghosting process. See Lawler Affidavit at ¶ 28.

that file by the operating system is called "file slack." File slack potentially contains information from past files stored in that area of the hard disk, or from temporary files used by the computer to store information in order to perform its tasks.

Pursuant to 28 U. S. Code section 1746, I declare under penalty of perjury that the foregoing is true and correct. Executed on September 20, 2002.


Donald Eugene Allison



U.S. Department of Justice

United States Attorney

Eastern District of Virginia

2100 Jamieson Avenue (703)299-3700
Alexandria, Virginia 22314

September 9, 2002

Frank W. Dunham, Jr.
Federal Public Defender
Eastern District of Virginia
401 Courthouse Sq., Ste. 300
Alexandria, VA 22314

Re: United States v. Zacarias Moussaoui; Crim. No. 01-455-A

Dear Mr. Dunham:

I write in response to your letter dated August 28, 2002, which you describe as a follow-up to the meeting on August 10, 2002. In this latest letter, you seek resolution of several discovery items. Below is a response to your request.

CDs

You list four CDs that you suggest either have no index or documents. As to CD marked MDLB_001, we have provided this CD to you twice, on June 25, 2002, and August 29, 2002. With respect to the CDs marked MHOB_003, 004, and 005, we produced an index for these items on July 15.

You also list CDs that you claim have images but no indexes. As noted in prior correspondence on this issue, many times we have described the contents of a CD in the letter that accompanies the production of that CD. Other times, we have provided an index after the CD has been provided, as a courtesy. Thus, for example, the CDs marked MFDN_001, MINS_001, MLBP_20000001, MLBR_001, M_PAN-70000001, and MTEL_001, 002 all were accompanied by letters that described the contents of the CDs.¹ The indexes to the CDs marked MBSC_008, 013,

¹ The descriptions are as follows:

MFDN_001 – 5/30/02 letter describes contents as EMS calls from 9/11
MINS_001 – 6/6/02 letter describes contents as INS records
MLBP_20000001 – 6/3/02 letter describes as photos
MLBR_001 – 6/4/02 letter describes as lab reports

Frank W. Dunham, Jr.

September 9, 2002

Page 2

014 and 105, and MSIB_001 were provided on July 15, 2002. The index was provided in a letter dated May 14, 2002, for MSLA, in a letter dated June 4, 2002, for MPGC_001, and in a letter dated August 29, 2002, for MRHA_001, and MSDC_009, 010. What remains is the group of CDs relating to the Afghanistan items, marked as MAFP_001, 007, 008, which are described as items obtained in Afghanistan.

In terms of the CD marked MLAC_001, the images missing are not discoverable, as noted in the attachment to the accompanying letter. The CD marked M1DS_20020724 was re-sent on August 14.

Finally, in terms of the CDs marked IAD, we have found a way to open and view the files. The solution is related to the video compression format used in various closed circuit TV (CCTV) products which are used to create surveillance tapes. The IAD video files are in an "AVI" video format and the FOURCC (Four Character Code) used to identify the video datastream format is "ADV1." We found information on compression formats at the following internet site: <http://www.fourcc.org/fccodec.htm>. This internet site provides links to various codecs compression format drivers that can be downloaded. Specifically, there is a link to the free Loronix Wavelet multimedia driver. By downloading and installing this driver on a computer, the videos can be viewed with a standard player such as Windows Media Player. The web site is: http://www.loronix.com/products/video_clips/wavecodec.asp. If after you download and install this multimedia driver and still have difficulty viewing the files, please let us know.

Hard Drives

You make several requests regarding the hard drives relating to the Moussaoui, Mukarram Ali and Afghanistan computers. With respect to some of the authenticating information you request, such as the BIOS information and other identifying information, we have previously provided this information in the form of the FBI 302s that describe the forensic analysis of each computer. For example, you recently received the analysis of the Toshiba Satellite 1700 laptop, model #PS170E-00021 EN, Serial # 11552157G, Barcode I11552157GSSS170-00021 ENS (which belonged to Moussaoui), and another computer. (See M-LBR_70002263 to M-LBR 70002265, which were copied on CD marked as MLBR_002).

M_PAN-70000001 – 8/28/02 letter describes as list of tenants of WTC.
MTEL_001, 002 – 7/8/02 letter describes as phone analysis by the FBI.

Frank W. Dunham, Jr.

September 9, 2002

Page 3

With respect to the 80 gigabyte hard drive, we have not copied multiple computer hard drives on a single hard drive, so we do not believe that you are mistaken on the amount of gigabytes of content on the hard drive your expert has examined. We already have provided the Huffman computer, but are unaware of any computer related to the Walker Sports Center.

We are not yet prepared to provide you with our view of the "significance" of the remaining computers. If you have a view as to the "significance" of any of these items, please so inform us.

Financial Records

You ask for the identification of the CDs containing bank records "linked" to the other 19 hijackers and any other person we consider to be a co-conspirator. We have provided the financial records that are discoverable, and we believe, the indexes that accompany most of the CDs produced to date. We believe that is more than sufficient for you to review the discovery materials.

Video/Audio Tapes

You ask for better copies of the videos marked as M-NT3-20000001 and M-WFB-200000032. Our copies are no better than your copies, so we have nothing of a higher quality to provide to you. However, if we enhance the quality of these tapes, we will provide you with copies of those enhanced tapes.

We are still working on the inventory of video and audio tapes that you provided to ascertain whether any of them contain either Rule 16 or *Brady* material. We trust that you are reviewing them yourselves to determine their significance to your defense.²

Translations

You express a concern about matching the translations with the other discovery items. With respect to the classified materials, we provided an index to you that matched the translations with the foreign language originals. Similarly, we have provided you with guidance on other translations. For example, the letters and indexes accompanying the transcriptions of the FDNY tapes were provided to you. As we continue to receive translations of additional documents, we will endeavor to provide a system that will enable you to match the translation with the original. In the meantime, if there are

² Under this category you once again ask for unredacted copies of the 302s. We have addressed this issue on several prior occasions and adhere to the views and the law previously discussed.

Frank W. Dunham, Jr.

September 9, 2002

Page 4

specific problems that you are having, please identify the items in question so that we can provide assistance.

Lab Reports

You express a concern about not having the "attachments" to the lab reports. However, we have provided photographs of the exhibits referred to in the lab reports (which are identified as "enclosures"). Moreover, we have provided you with a list of the "K" and "Q" items as labeled by the FBI lab, all of which can be electronically searched on the discovery CDs we have provided.

With respect to summaries of the expected expert testimony, we note that we already have provided you with the lab reports prepared by the FBI experts, as well as their cv's. We will provide you with summaries of the expected testimony of the experts we intend to call as witnesses at a later date.

Miscellaneous

The telephone number referred to in Overt Act 63 is 49 175 953 1540. The number for the stolen German passport of Ahad Sabet is Z7567858. We will provide you with an estimate of the expected amount of Jencks Act material at a later date.

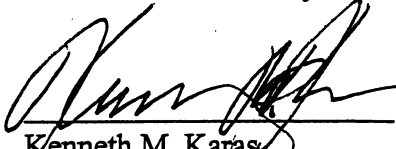
Defense Discovery

As we mentioned to you on a previous occasion, we have yet to receive a single item of discovery from the defense. We are perplexed by this given that the case has been under indictment for ten months, and hereby request that you provide the discovery items to which we are entitled forthwith.

Sincerely,

Paul J. McNulty
United States Attorney

By:


Kenneth M. Karas
Assistant U.S. Attorney

cc: Zacarias Moussaoui

REDACTED

UNDER SEAL

DOCUMENTS UNDER SEAL

DOCUMENTS UNDER SEAL

DOCUMENTS UNDER SEAL